

Figure. 1. Typical usage of a stream cipher  
PRIOR ART

200

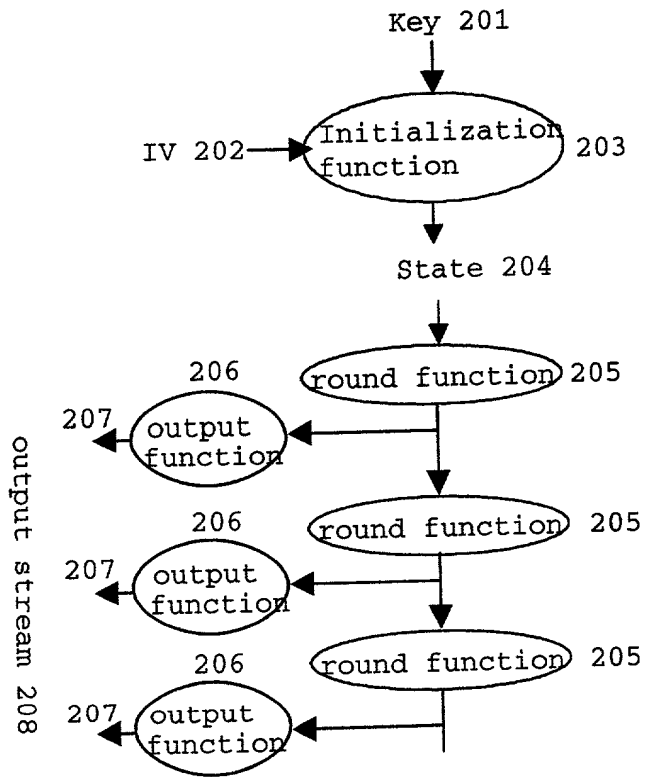


Figure 2. Structure of a typical stream cipher  
PRIOR ART

300

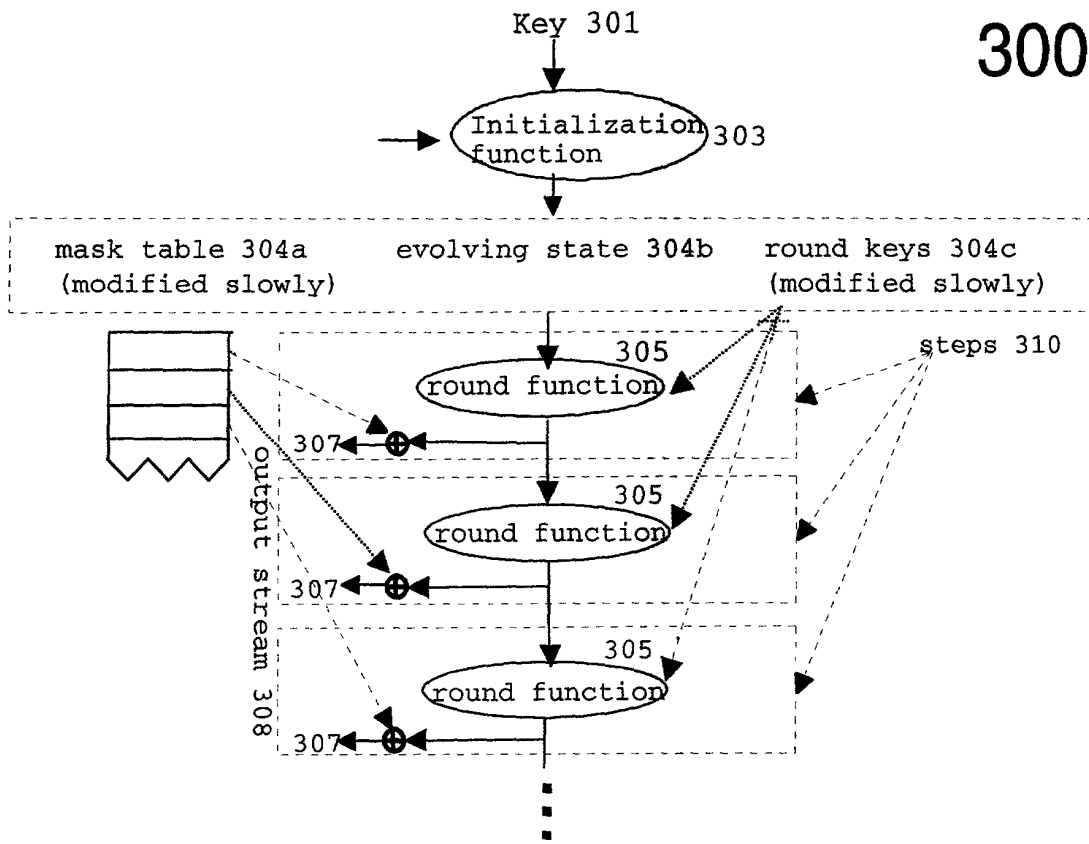


Figure 3

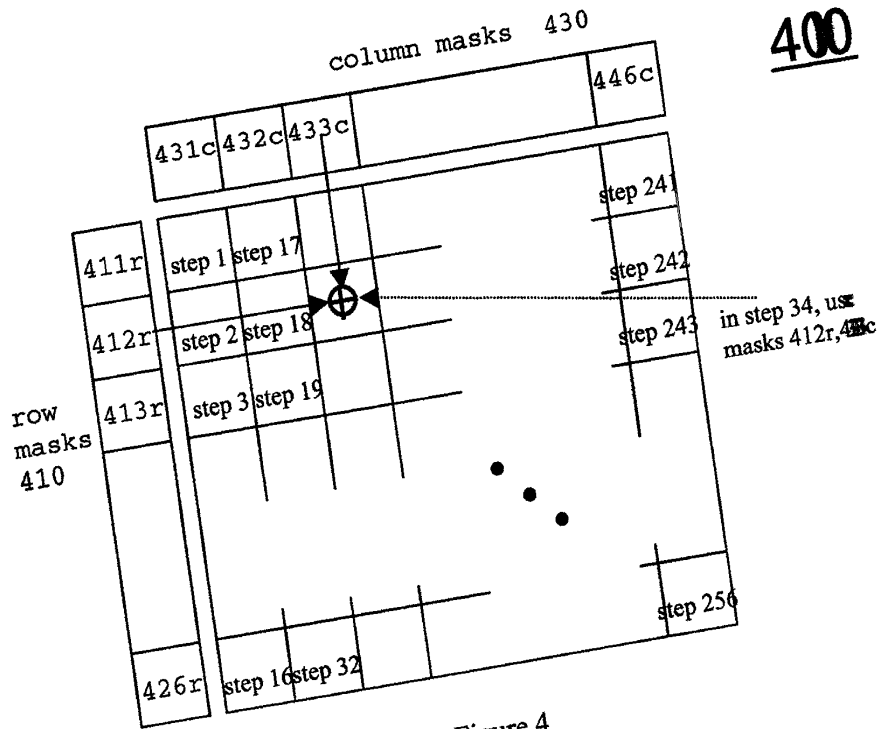


Figure 4

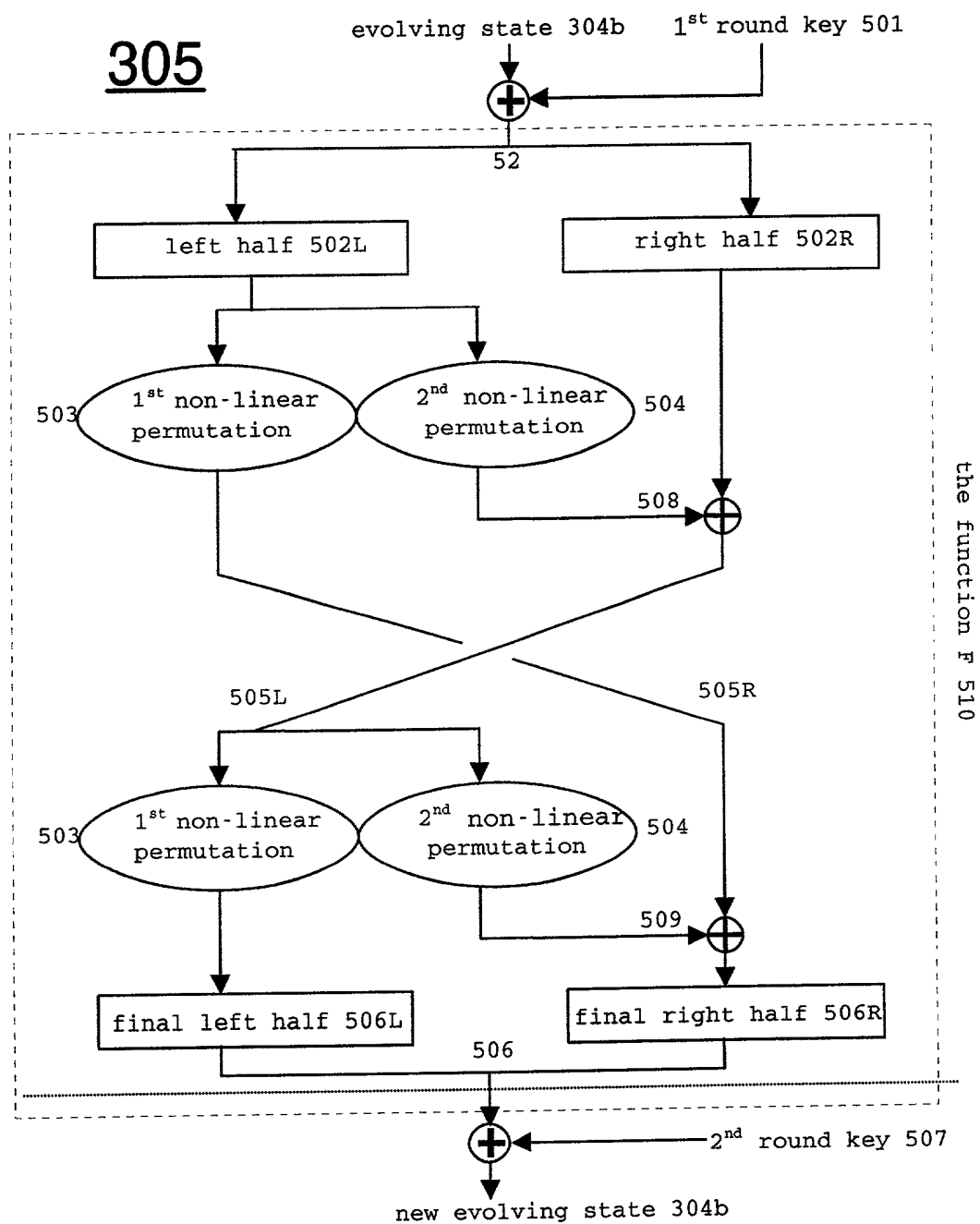


Figure 5

$$610 \begin{pmatrix} a & c & e & g \\ b & d & f & h \end{pmatrix}$$

600

byte substitution 601

replace each byte x  
by S[x]

$$602 \begin{pmatrix} S[a] & S[b] & S[c] & S[d] \\ S[b] & S[d] & S[f] & S[h] \end{pmatrix}$$

row shift 603

rotate the second row  
by one byte to the right

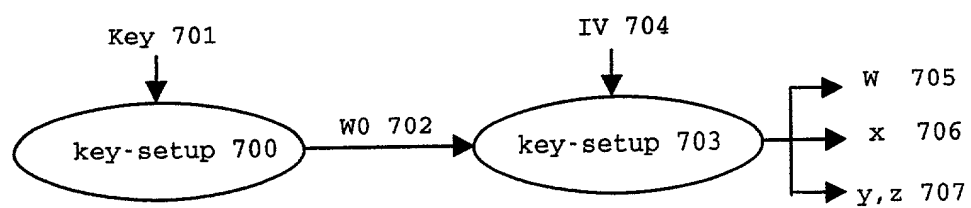
$$604 \begin{pmatrix} S[a] & S[b] & S[c] & S[d] \\ S[h] & S[b] & S[d] & S[f] \end{pmatrix}$$

column mix 605

replace each column c  
by M \* c

$$606 \begin{pmatrix} a' & c' & e' & g' \\ b' & d' & f' & h' \end{pmatrix}$$

Figure 6



202, 302

Figure 7